APPROVED	RESPONSIBILITY	EFFECTIVE DATE	NUMBER	PAGE
	Information Technology Administrator (HIPAA Security Officer)	12/2004	6420-27	1 of 2

TITLE: TESTING AND REVISION PROCEDURES POLICY

PURPOSE:

The purpose is to implement procedures for periodic testing and revision of contingency plans. This is a standard required under the Administrative Safeguards of the HIPAA Security Rule.

SCOPE:

This policy applies to Guam Memorial Hospital Authority in its entirety, including all workforce members. Further, the policy applies to all systems, network, and applications that process, store or transmit ePHI.

POLICY:

Testing and revision procedures are procedures for processing of periodic testing of written contingency plans to discover weaknesses and the subsequent process of revising the documentation and procedures, if necessary. These written testing and feedback mechanisms are the key to successful testing.

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, must ensure that procedures for testing and revision address the following:

- Sufficient awareness and training of all affected personnel on how to react in the event of a disaster or other business interruption.
- Validation of the Disaster Recovery and Emergency Mode Operation Plan to ensure that processes and procedures are effective.
- Identification of weaknesses in the Disaster Recovery and Emergency Mode Operation Plan and procedures to mitigate identified weaknesses.
- Procedures to ensure that Disaster Recovery and Emergency Mode Operation Plan remain current and active.
- Procedures that test interdependencies among critical business processes, applications, and systems.
- Procedures that test the adequacy of equipment in place to fulfill Disaster Recovery and Emergency Mode Operation Plan.
- Periodic updates and testing of all procedures and components of the Disaster Recovery Plan and Emergency Mode Operation Plan.

Reviewed: 01/2006
Revised: 02/2006
Approved: EMC 2/15/06

RESPONSIBILITIES:

The HIPAA Security Officer, under the delegated authority of the Hospital Administrator, will be responsible for implementing the requirements of Testing and Revision Procedures.

COMPLIANCE:

Failure to comply with this or any other security policy will result in disciplinary actions as per the Sanction Policy 6420-8. Legal actions also may be taken for violations of applicable regulations and laws such as HIPAA.

Testing and Revision Procedure is an addressable implementation specification defined within the Contingency Plan standard (164.308 (a)(7)) in the Administrative Safeguards category of the HIPAA Security Rule.

PROCEDURES:

Procedures related to the Testing and Revision Procedures standard include:

- Data backup
- Disaster recovery
- Emergency mode operations
- Applications and data criticality analysis

REFERENCES:

- HIPAA Final Security Rule, 45 CFR Parts 160, 162, and 164, Department of Health and Human Services, http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/default.asp, February 20, 2003.

- CMS, "CMS Information Systems Security Policy, Standards and Guidelines Handbook", CMS, February 2002.

- International Standards Organization (ISO/IEC 17799:2000(E)).